

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Chad Preston Pupillo, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), and I am an investigator or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered to conduct investigations of, and to make arrests for, the offenses enumerated in Title 18, 19, 21, 31 United States Code and other related offenses. The affiant has been employed as a federal agent since March 2009 and has focused on investigations involving violent crime, violent street gangs, terrorism, and national security. Your affiant is currently assigned to Safe Streets/ Gang Task Force in the Charlotte, North Carolina FBI office. Through investigations and training, your affiant has become familiar with the methods and schemes employed by violent street gangs in support of racketeering activities.

2. This affidavit is submitted in support of an application, pursuant to Rule 41 of the Federal Rules of Criminal Procedure, for a search warrant for the following electronic devices seized on May 18, 2012 and which have been and continue to be in the possession of the FBI:

DEVICE

IDENTIFYING SERIAL NUMBER, MODEL NUMBER, etc.

- | | |
|--|--------------------|
| <ul style="list-style-type: none">• iPhone | FCC ID: BCG-A1303B |
|--|--------------------|

and the electronic data contained therein. The above-described electronic devices are currently stored at the FBI Charlotte Field Office located within the Western District of North Carolina.

The devices have been stored in a manner in which the contents are, to the extent material to this investigation, in substantially the same state as they were when the devices first came into the possession of the FBI.

3. I have participated in the investigation as related in this affidavit. As a result of the affiant's participation in this investigation and information provided by agents/officers from other FBI offices, your affiant is familiar with aspects of this investigation. On the basis of this familiarity, and on the basis of the other information that the affiant has reviewed and found to be reliable, it is alleged that there is probable cause to believe that the above described electronic devices, contain stored electronic information and images relating to a criminal organization, namely the United Blood Nation a criminal street gang, and the nature and scope of the conspiracy.

4. Based on my training and experience, I am familiar with the ways in which members of criminal organizations conduct their business via electronic devices, to include but not limited to:

- a. Gang members commonly use electronic communication devices to communicate with other members of their organization. In fact, electronic communication devices are considered a "tool of the trade" as gang members often have multiple electronic communication devices to give or receive instructions as they complete gang business and drug transactions. Gang members are aware that it is much more difficult for investigators to identify and link a specific electronic communication device to them as opposed to a fixed or hard line electronic communication device. It is also common for gang members to utilize electronic communication devices registered in nominee names. This enables them to

conduct gang business and illegal drug trafficking activities by electronic communication devices, with less of a chance of being identified.

- b. Electronic communication devices have the capability of storing numerous telephone numbers of other individuals. This feature is commonly referred to as "Speed Dialing." Electronic communication devices also can have "Caller Id", "email" and "Text Messaging" features on the telephones. "Caller Id" identifies the telephone numbers of the incoming calls. Email and Text Messages can be stored on the cellular telephone and also identifies whom the message was sent to or whom it came from. In addition, electronic communication devices have the capability of recalling past telephones numbers dialed. In addition to enabling voice communications, wireless telephones now offer a broad range of capabilities. These capabilities include, but are not limited to: storing names and phone numbers in electronic "address books", sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system technology for determining the location of the device.
- c. Gang members take, or cause to be taken, photographs or videos of themselves and their associates, property derived from the distribution of narcotics, weapons, and their products, and such media is often kept in their electronic communication devices.

- d. Gang members commonly utilize electronic communication devices equipped with SMS text messaging and electronic mail messaging to communicate with other gang members and drug traffickers. These features are frequently used in order to remain anonymous by communicating via text as opposed to voice, therefore further avoiding detection by law enforcement.
- e. Gang members commonly utilize electronic communication devices equipped with certain computer programs/applications to store electronic data concerning their gang organization and their drug trafficking activities. An example of this would be a data base/spreadsheet application such as "Excel". These programs are frequently used in order to maintain a memorialized record of gang members and records of their dues, past drug transactions and the amount of money owed and paid by customers and the monies owed to the suppliers of the narcotics.
- f. Based upon my research, training and experience, as well as conversations with other law enforcement personnel within the FBI who have experience with GPS/GNS devices, I know the following. Drug traffickers commonly use electronic Global Positioning Systems or GPS mapping devices (commonly referred to as "a GPS") to locate locations to meet other co-conspirators, narcotics stash locations and narcotics drop-off locations. The GPS is a space-based radio navigation system consisting of a constellation of satellites and a network of ground stations used for monitoring and control. A minimum of 24 GPS satellites orbit the Earth at an altitude of approximately 11,000 miles providing users with accurate information on position, velocity, and time anywhere in the world and in all weather conditions. The GPS/GNS devices located on the subject airplane use

global positioning satellites to track and record the location of the devices, and therefore, the location of any object to which they are attached. The GPS systems utilized in this instance also contain a "backtrack" feature that displays or graphs the journey. Thus, there is probable cause to believe that the GPS devices will contain recorded evidence of the physical location of the airplane and the vehicle whenever they were in operation. Information and evidence of these travels should be helpful in identifying the locations and contacts related to the drug distribution conspiracy.

- g. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device and can store information for long periods of time. Even when a user deletes information from a device, it can sometimes be recovered with forensic tools.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

6. This investigation targets the United Blood Nation (UBN) and alleges that the UBN, including its leadership, members and associates, constituted an "Enterprise" as defined in Section 1961(4) of Title 18, United States Code, that is, a group of individuals associated in fact. The Enterprise constituted an ongoing organization whose members functioned as a continuing

unit for the common purpose of achieving the objectives and purposes of the Enterprise. The Enterprise was engaged in, and its activities affected, interstate and foreign commerce.

7. The investigation alleges that UBN members in North Carolina and elsewhere engaged in criminal activity, including, but not limited to, attempted murder, aggravated assault, robbery, attempted robbery, drug trafficking, firearms trafficking, firearms possession, and conspiracy to commit these crimes.

8. Additionally, this investigation concerns allegations that the operator of the electronic device used wireless communications and the internet to promote, manage, and facilitate the UBN criminal enterprise, and to distribute gang information, documentation, and records to members of the criminal enterprise located in North Carolina and elsewhere.

9. On or about July 7, 2011 SAMANTHA WILLIAMS aka "Samantha Wilkinson" aka "Lady Sam" set up a meeting between ALAN BARNETT aka "Big Al", KEMMEY NICOLE COOKE aka "Gangsta Wu", and DARYL WILKINSON aka "OG Powerful" in New York about the UBN enterprise. WILLIAMS utilized telephone number (347) 439-1475 to contact BARNETT and others in order to accomplish this task, which was captured during court-authorized Title III interceptions.

10. On or about August 22, 2011, WILKINSON advised WILLIAMS to tell a ranking member of the UBN that the UBN Council did not support FRANKLIN ROBBS, aka "Frankie Boo", that the ranking member of the UBN needed to "step up", that those under ROBBS were now under the ranking member of the UBN, and that ROBBS was demoted.

11. On or about August 22, 2011, WILLIAMS advised WILKINSON that a ranking member within the UBN was not happy about her telling him that WILKINSON said he should have consulted with him first about ROBBS.
12. On or about August 24, 2011, WILKINSON advised WILLIAMS that a ranking member within the UBN needed to know that he should have never told ROBBS that he had permission to open the books to allow a local non-affiliated gang to become a member of the UBN under his command, that she should tell ROBBS that anyone claiming the local non-affiliated gang was “on the plate”¹, and that the issue created by ROBBS made it before the UBN Council².
13. On or about August 28, 2011, WILKINSON advised WILLIAMS that she needed to let the ranking member within the UBN know that he needed to be more active and that he needed to consult with him [WILKINSON] in order to know what is going on within the UBN and in what direction they [the UBN] are headed.
14. On May 5, 2012, a Confidential Human Source (CHS) forwarded an email which contained the email address MISSSAM1121@AOL.COM. According to CHS, this email was utilized by SAMANTHA WILLIAMS for communicating and directing UBN gang business and advised that WILLIAMS used MISSSAM1121@AOL.COM to communicate messages to UBN gang members which WILLIAMS received from DARYL WILKINSON.
15. On February 6, 2013, an administrative subpoena was filed with cellular service provider AT&T for subscriber information pertinent to telephone number (347) 439-1475. AT&T

¹ “On the plate” is a term used within the UBN to describe a member who is targeted for severe punishment or death.

² The UBN Council is a group of leaders from the various sets, or membership groups, of the UBN. The Council makes the ultimate decisions concerning the gang, gang rules, and gang protocols.

responded with a copy of subscriber information which listed the financially liable party as ROOSEVELT MCFARLAND living at 1420 PROSPECT AVENUE APARTMENT 3D, BRONX, NEW YORK. The response stated that MCFARLAND had been a customer since 2005 and listed the home telephone for the party as (718) 861-0449. The AT&T response further listed two contact emails for the subscriber, SWILLIAMS@ODYSSEYHOUSEINC.ORG and MISSSAM1121@AOL.COM. Samantha Williams was, prior to her arrest, employed at Odyssey House. Both email addresses which were listed as the email address of the subscriber to the phone service are used by and attributable to SAMANTHA WILKINSON.

16. New York Department of Corrections provided the FBI with several hundred letters written by WILKINSON. Several letters were identified as communications between WILKINSON and WILLIAMS. WILKINSON addressed the letters to SAMANTHA WILKINSON, 1420 PROSPECT AVENUE APARTMENT 3D, BRONX, NY 10459. When the letters were sent from WILLIAMS to WILKINSON, the return address used was MRS. S WILKINSON, 1420 PROSPECT AVENUE #3D, BRONX NY, 10459.

17. On May 18, 2012, WILLIAMS was arrested pursuant to a Federal Arrest Warrant. She was located and the arrest was effected at 1420 PROSPECT AVENUE, APT 3D, BRONX, NEW YORK. During the arrest of WILLIAMS, arresting agents seized WILLIAMS' iPhone bearing FCC ID BCG-A1303B. On arrest paperwork, WILLIAMS provided her home telephone number as (718) 861-0449 and provided her cellular telephone number as (347) 439-1475.

18. Since the time of her arrest, the iPhone has been maintained by the Federal Bureau of Investigation in a locked evidence facility and has not been altered in any way.

TECHNICAL BACKGROUND

19. The iPhone is a line of smartphones designed and marketed by Apple Inc. It runs Apple's iOS mobile operating system, known as the "iPhone OS" until mid-2010, shortly after the release of the iPad. The first iPhone was released on June 29, 2007; the most recent iPhone, the sixth-generation iPhone 5, on September 21, 2012. The user interface is built around the device's multi-touch screen, including a virtual keyboard. The iPhone has Wi-Fi and cellular connectivity (2G, 3G and 4G).

20. An iPhone can shoot video (though this was not a standard feature until the iPhone 3GS), take photos, play music, send and receive email, browse the web, send texts, and receive visual voicemail. Other functions—games, reference, GPS navigation, social networking, etc.—can be enabled by downloading apps; as of 2012, the App Store offered more than 775,000 apps by Apple and third parties.

21. There are six generations of iPhone models, each accompanied by one of the six major releases of iOS. The original iPhone was a GSM phone, and established design precedents, such as a button placement that has persisted through all models and a screen size maintained until the launch of the iPhone 5 in 2012. The iPhone 3G added 3G cellular network capabilities and A-GPS location. The iPhone 3GS added a faster processor and a higher-resolution camera that could record video at 480p. The iPhone 4 featured a higher-resolution 960 × 640 "retina display", a higher-resolution rear-facing camera and a lower-resolution front-facing camera for video calling and other apps. The iPhone 4S added an 8-megapixel camera with 1080p video recording, a dual-core processor, and a natural language voice control system called Siri. iPhone

5 features the new A6 processor, holds a 4-inch Retina display that is larger than its predecessor's 3.5-inch display, and replaces the 30-pin connector with an all-digital Lightning connector.

22. The Wi-Fi feature enables use of any Wi-Fi network, including over 20,000 Wi-Fi hotspots at various places such as retail establishments (e.g. Starbucks) and public places (e.g. airports).

The iPhone has video, audio, photo and document display capabilities which enable the device to send/receive videos, audio files, photos and written documents in multiple formats such as pdf.

23. It is believed that records might be found stored on the iPhone's hard drive or other storage media. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis.

24. I submit there is probable cause to believe records are stored in that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being

used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

25. As further defined in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described, but also for evidence that establishes how computers were used, the purpose of their use, who used them, and when. Some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), computer storage media can

contain other forms of electronic evidence as well, and such it is requested that the following be included in the search:

- a. Forensic evidence of how computers were used, the purpose of their use, who used them, and when, is, as described further in Attachment B, called for by this warrant. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a computer or storage medium regarding who has used or controlled the computer or storage medium. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed

dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

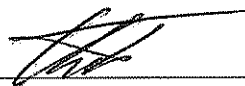
- c. The presence or absence of counter-forensic programs (and associated data) that are designed to eliminate data may be relevant to establishing the user's intent. To investigate the crimes described in this warrant, it might be necessary to investigate whether any such malicious software is present, and, if so, whether the presence of that malicious software might explain the presence of other things found on the storage medium. I mention the possible existence of malicious software as a theoretical possibility, only; I will not know, until a forensic analysis is conducted, whether malicious software is present in this case.
- d. A suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime.

CONCLUSION

26. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the electronic devices there exists evidence of the crimes previously set forth in this affidavit. Accordingly, a search warrant is requested.

27. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,



Chad Preston Pupillo
Special Agent
Federal Bureau of Investigation (FBI)

Sworn to and subscribed before me, this the 27th day of March, 2013.



DAVID C. KEESLER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

- I. This warrant applies to an Apple iPhone bearing FCC ID BCG-A1303B.

ATTACHMENT B

PARTICULAR THINGS TO BE SEIZED

I. Information and materials to be seized from the electronic device identified in Attachment A:

a. The contents of all e-mails stored on the electronic device, including copies of e-mails sent to and from accounts maintained on the device, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information stored on the electronic device, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register any accounts, log-in IP addresses associated with session times and dates, account statuses, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payments (including any credit or bank account number stored on the electronic device);

c. GPS location data stored on the electronic device and used in conjunction with device software and applications;

d. All records or other information stored by an individual using electronic device, including address books, contact and buddy lists, calendar data, pictures, and files;

II. Information to be seized by the government;

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of knowingly and intentionally conspiring to conduct and participate, directly and indirectly, in the conduct of the affairs of the Enterprise through a pattern of racketeering activity, as defined in 18 U.S.C. §§ 1961(1) and (5) involving the use of the iPhone, including, for each electronic device listed on Attachment A, information pertaining to the following matters:

- a. Murder chargeable under North Carolina Gen. Stat. §§ 14-17 and 14-2.4;
 - b. Bribery chargeable under North Carolina Gen. Stat. §§ 14-217, 14-218 and 14-2.4; and
 - c. Robbery chargeable under North Carolina Gen. Stat. §§ 14-87.1, 14.87 and 14-2.4;
- and multiple acts involving:
- d. The felonious manufacture, importation, receiving, concealment, buying, selling or otherwise dealing in a controlled substance, in violation of 21 U.S.C. §§ 841 and 846; and
 - e. The illegal use of a communication facility, in violation of 21 U.S.C. §843(b);
- and multiple acts indictable under:
- f. 18 U.S.C. § 1951 (Interference with commerce, robbery or extortion).